線形符号の重み分布 (群論と組み合せ論)

AUTHOR(S):

嵩, 忠雄

CITATION:

嵩, 忠雄. 線形符号の重み分布 (群論と組み合せ論). 数理解析研究所講究録 1973, 178: 79-90

ISSUE DATE:

1973-05

URL:

http://hdl.handle.net/2433/107102

数理解析研究所講究録
178巻 1973年 79-90

線形符号の重み分布

大阪大　基礎工　　嵩　忠雄

1. Mattson-Solomon多項式[1,2,3]と多項式符号[1,2]

巡回符号の表現法にMattson-Solomon多項式（以下，MS多項式と略記）を使う方法がある．qをある素数のべき乗，mを整数，nをq^m-1をわり切る正整数，Cをq元(n,k)巡回符号，βを$GF(q^m)$の位数nの元とする．符号ベクトル$(v_0, v_1, \cdots, v_{n-1}) \in C$について，$v(X)=v_0+v_1X+\cdots+v_{n-1}X^{n-1}$とおく．$v$についてのMS多項式，$MS(v,X)$をつぎのように定義する．

$$MS(v,X)=n^{-1}\sum_{j=1}^{n} S_j X^{n-j} \qquad (1)$$

ここで，　$S_j=v(\beta^j)$，

このとき，

$$MS(v,\beta^l)=n^{-1}\sum_{j=1}^{n} S_j \beta^{-jl}=n^{-1}\sum_{j=1}^{n}\beta^{-jl}\sum_{i=0}^{n-1} v_i \beta^{ij}$$

$$=n^{-1}\sum_{i=0}^{n-1} v_i \sum_{j=1}^{n}\beta^{(i-l)j},$$

$\sum_{j=1}^{n}\beta^{(i-l)j}$ は $i\neq l$ のとき 0，$i=l$ のとき n ゆえ，

$$MS(v, \beta^l) = v_l \qquad (2)$$

すなわち，$\beta^1, \beta^2, \cdots, \beta^n$ のなかで，$MS(v, X)$ の根である元の個数を r とすれば，v の重み $w(v)$ は $n-r$ に等しい。

C の生成多項式を

$$g(X) = \prod_{i \in R} (X - \beta^i)$$

$R \subseteq \{0, 1, \cdots, n-1\}$，$R$ は $\{0, 1, \cdots, n-1\}$ の置換 $\pi_q : i \to qi \pmod n$ に不変．R に属さない最小正整数を d_{BCH} とすると，$g(X) \mid v(X)$ より*，

$$S_j = v(\beta^j) = 0, \quad j \in R \qquad (3)$$

したがって，$MS(v, X)$ の次数は高々 $n - d_{BCH}$．(2) より，v が 0 ベクトルでないとき，その重み $w(v)$ は，

$$w(v) \geq d_{BCH} \qquad (4)$$

この d_{BCH} は最小重みに関する BCH 下界に他ならない．

$v_i \in GF(q)$ より，

$$S_j^q = v(\beta^j)^q = v(\beta^{qj}) = S_{qj} \qquad (5)$$

逆に，$S_j = 0$ $(j \in R)$，$S_j^q = S_{qj}$ $(1 \leq j \leq n)$ を満すように，$GF(q^m)$ の元の組，$(S_1, \cdots, S_n)$ を任意に選び，

$$a(X) = n^{-1} \sum_{j=1}^{n} S_j X^{n-j},$$

$$v_a = (a(\beta^0), a(\beta^1), \cdots, a(\beta^{n-1}))$$

とおくと，(2)同様

$$v_a(\beta_j) = S_j, \quad 1 \leq j \leq n$$

* S_j の添字は mod n で考える．

すなわち，$v_a \in C$ かつ，

$$MS(v_a, X) = a(X).$$

このことは，一定の条件を満足する多項式の集合Fを与え，各多項式 $f \in F$ に対して，変数に一定の仕方で値を代入したときのfの値を並べたベクトルを対応させ，このようにして得られたベクトル全体で符号を定義する方法の一例である．Mullerによる Reed-Muller符号[1,2]の導入は，その最初の例である．

$GF(q)$ の上の ν 次以下の m 変数の多項式全体の集合を $P_{\nu,m}$ とかく．$GF(q^m)$ の原始元の一つを α とする．

$$\alpha^i = \sum_{j=0}^{m-1} a_{ij}\alpha^j, \quad 0 \le i < q^m - 1.$$

ここで，$a_{ij} \in GF(q)$.

$f(x_1, \cdots, x_m) \in P_{\nu,m}$ について，$f(a_{i0}, a_{i1}, \cdots, a_{im-1})$ を簡単のため，$f(\alpha^i)$ と，$f(0, \cdots, 0)$ を $f(0)$ とかき，

$$v_f^e = (f(0), f(\alpha^0), f(\alpha^1), \cdots, f(\alpha^{q^m-2}))$$

とおく．v_f^e から，最初の成分を除いたものを v_f とかく．

$\{v_f \mid f \in P_r\}$ を<u>長さ $n = q^m - 1$ の q 元 ν 次GRM符号</u>（generalized Reed-Muller code）という．v_f の代りに，v_f^e をとったとき，e-GRM符号（extended GRM code）という．$q=2$ のとき，e-GRM符号を<u>RM符号</u>（Reed-Muller code）とよぶ．この定義は，成分の順序を除いて，Mullerのそれに等しい．また，$m=1$ のとき，GRM

符号をＲＳ符号(Reed-Solomon code)という．ν次RS符号はMS多項式の集合が$P_{\nu,1}$に一致するから，$d_{BCH}=n-\nu$，生成多項式は，$g(X)=\prod_{i=1}^{d_{BCH}-1}(X-\alpha^i)$．情報点数$k=n-d_{BCH}+1$．一方最小重み$d\leq n-k+1=d_{BCH}$．(4)より，$d=d_{BCH}$．$q=2^s$のとき，GF(q)の各元をGF(2)のｓ字組で表わすと，q元ＲＳ符号から，２元$(s(q-1),\ s(\nu+1))$符号が得られる．密集した誤り訂正に有用であり，また最近，Justesen符号の外部符号として利用されている．

なお，ν次e-GRM符号の双対符号は$((q-1)m-\nu-1)$次e-GRM符号である．整数$0\leq i<q^m$について，$i=\sum_{j=0}^{m-1}c_j q^j$，$0\leq c_j<q$とする．このとき，

$$W_q(i)=\sum_{j=0}^{m-1}c_j$$

とおく．長さq^m-1のν次GRM符号は巡回符号であり，その生成多項式$g(X)$は，[1]

$$g(X)=\prod_{\substack{0<i<q^m-1\\ 0<W_q(i)<(q-1)m-\nu}}(X-\alpha^i)$$

$q=q_0^s$とし，q元符号Cにおいて，すべての成分がGF(q_0)の元であるような符号ベクトル全体の集合C_0を符号Cの<u>部分体GF(q_0)の部分符号</u>という．Cが$g(X)=\prod_{i\in R}(X-\alpha^i)$を生成多項式とする巡回符号のとき，$C_0$も巡回符号であり，その生成多項式は，$g_0(X)=\prod_{i\in R_0}(X-\alpha^i)$，ここで$R_0$はRを含み，$\pi_{q_0}$で不変な最小な集合である．さらに，$n_0$がnをわり切るとき，符

号長nの符号Cの符号ベクトルのなかで，残りの成分が最初のn_0成分の周期的くり返しであるようなもの全体を考えると，各ベクトルの最初のn_0成分からなるベクトルの集合は，長さn_0の符号となる．n_0をq^m-1の約数として，このようにしてGRM符号の部分体部分符号より得られる長さn_0の符号を多項式符号[1]（polynomial code）という．

ＢＣＨ符号は多項式符号であり，狭義のＢＣＨ符号はＲＳ符号の部分体部分符号である．多くの重要な符号のクラスは多項式符号かその双対符号である．

2. Carlitz-Uchiyama の上界の応用[3]

$q=2$，すなわち２元で符号長$n=2^m-1$，設計距離$d_{BCH}=2t+1$のＢＣＨ符号の双対符号Cを考える．もとのＢＣＨ符号の生成多項式は$\prod_{i\in R}(X-\alpha^i)$，ここで$\alpha$は$GF(2^m)$の原始元，$R$は$\{1,2,\cdots,2t\}$を含み，$\pi_2$で不変な最小の集合である．したがって，$C$の生成多項式は，$g(X)=\prod_{i\in\{0,1,\cdots,n-1\}-R}(X-\alpha^{-i})$である．$v\neq 0\in C$とすると，

$$MS(v,X)=\sum_{j=1}^{n}S_jX^{n-j}=\sum_{j=0}^{n-1}S_{n-j}X^j=\sum_{j\in R}S_{n-j}X^j$$

ここで，$S_j^2=S_{2j}$，　$1\le j\le n$　　(6)

Rをπ_2のサイクルに分割し，それぞれの代表として，$2t-1$以下の非負整数を選び，それらを$j_1,\cdots,j_\mu$とかく．j_iの属す

るサイクルの長さをm_iとする．$2t-2 < 2^{m/2}$と仮定すると，$m_i = m$．（もし，$m/m_i \geq 2$とすると，$(2^{m_i}-1)j_i \leq (2^{m/2}-1)(2t-1) < 2^m - 1$となり，$\alpha^{j_i(2^{m_i}-1)} = 1$に矛盾）このとき，(6)より，

$$v_\ell = MS(v, \alpha^\ell) = \sum_{i=1}^{\mu} T_r(S_{n-j_i}\alpha^{j_i\ell}) = T_r\left(\sum_{i=1}^{\mu} S_{n-j_i}\alpha^{j_i\ell}\right) \quad (7)$$

ここで，$T_r(X) = X + X^2 + \cdots + X^{2^{m-1}}$

$\varphi(X) = \sum_{i=1}^{\mu} S_{n-j_i} X^{j_i}$ とおくと，$\varphi(X)$の次数は$2t-1$以下．

定理（Carlitz - Uchiyama）：αを$GF(2^m)$の原始元，$f(X)$を$GF(2^m)$の上の次数νの多項式で，標数2の有限体の上のどのような多項式$r(X)$についても，$[r(X)]^2 - r(X) - s(X)$が定数とならないとき，

$$\left| (-1)^{T_r(f(0))} + \sum_{i=0}^{2^m-2} (-1)^{T_r(f(\alpha^i))} \right| \leq (\nu-1)2^{m/2}.$$

上の$\varphi(X)$は定理の条件を満す．(7)より，$v_\ell = T_r(\varphi(\alpha^\ell))$．故に$\left| 1 + \sum_{\ell=0}^{n-1}(-1)^{v_\ell} \right| = |1 + n - 2w(v)| \leq (2t-2)2^{m/2}$．したがって，$w(v) \geq 2^{m-1} - (t-1)2^{m/2}$．まとめて*，

「符号長2^m-1，設計距離$2t+1$の2元（狭義）BCH符号の双対符号の最小重みは少くとも

$$2^{m-1} - (t-1)2^{m/2}$$ 」

3. 重み分布

符号この重みiをもつ符号語の数をA_iとかくことにする．

* $2t-2 \geq 2^{m/2}$なら，自動的に成立．

$A(Z)=\sum_{i=0}^{n} A_i Z^i$ を C の weight enumerator（以下 WE と略記）という．同じ WE をもちかつ等価*でない符号の存在が知られているが[2]，WE は符号の構造に関する重要なパラメータであり，また C が 2 元線形符号で最小重みが $2t+1$ 以上のとき，誤り確率 P_0 の 2 元対称通信路において t 重以下の誤り訂正符号として使う場合，間違って復号する確率 Q は，多項式

$$P_n(Z)=(1-P_0+P_0Z)^n A((Z-P_0Z+P_0)/(1-P_0+P_0Z))$$

から，$t+1$ 次以上の項を除いて得られる多項式を $P_t(Z)$ とおくとき，$Q=P_t(1)-\sum_{i=0}^{t}\binom{n}{i}P_0^i(1-P_0)^{n-i}$ で与えられる[2,3]．

MacWilliams の等式[1,2,3]：GF(q) の上の線形 (n,k) 符号 C の WE を $A(Z)$，C の双対符号 C_d の WE を $B(Z)$ とすると，

$$q^{-k}(1+(q-1)Z)^n A\left(\frac{1-Z}{1+(q-1)Z}\right)=B(Z) \qquad (8)$$

双対符号 C_D と等価な符号 C を自己双対という．C が自己双対のとき，(8) で $A(Z)=B(Z)$ 故，可能な $A(Z)$ の形は著しく制限される．$A(Z)$ の代りに，$W(X,Y)=\sum_{i=0}^{n} A_i X^{n-i}Y^i$ を使うと，

$$W(X,Y)=W\left(\frac{X+(q-1)Y}{\sqrt{q}},\ \frac{X-Y}{\sqrt{q}}\right)$$

これから，たとえば，$q=2$ かつ奇数の重みをもつ符号ベクトルが存在しないとき，

$$W(X,Y)=\sum_{2i+8j=n} C_{ij}(X^2+Y^2)^i[X^2Y^2(X^2-Y^2)^2]^j$$

の形で与えられる[4]．これの拡張について，文献(5,13)が詳しい．

* ベクトルの成分の位置かある置換により，C_1 から C_2 が得られるとき，両者を等価という．

RS符号のWEは知られている.[1,2,13] それ以外，重み分布についての主な結果は2元符号に関するもの故，以下$q=2$とする.

(i) Cを(n,K)線形符号として，$(n+1, K)$線形符号，

$$C_e=\{(\sum_{i=1}^{n} v_i, v_1, \cdots, v_n) \mid (v_1, \cdots, v_n) \in C\}$$

をCの拡張符号(extended code)という．C_eは重みが奇数の符号ベクトルをもたない．nが奇数でCが巡回符号とする．C_eは符号ベクトル$(1,1,\cdots,1)$を含むから，C_eの重みiの符号ベクトルの数をA_i^eとすると，$A_i^e=A_{n+1-i}^e$ $(0\leq i\leq n+1)$．C_eが成分の位置に関するある2重可遷置換群について，不変ならば(たとえば，多項式符号，したがってBCH符号，平方剰余符号などはそうである)，

$$A_{2i-1}=2iA_{2i}^e/(n+1)=2iA_{2i}/(n+1-2i)$$

が成立する.[1,2,3] したがって，A_{2i}^e あるいはA_{2i}を知れば十分である.

(ii) 重みの制限：一定の条件を満すi以外$A_i=0$であるといった形の結果が若干知られている.[2,3]

(ii,1) (McEliece)：Cを巡回符号，そのパリティ検査多項式がj $(0<j<K)$について，j個以下(重複を許す)の根を任意にえらんだとき，その積がいつも1にならないならば，すべての符号ベクトルの重みは2^jでわり切れる.

(ii.2) 長さ 2^m の2次RM符号の符号ベクトルの重みは，

$$2^{m-1} + \varepsilon 2^{i-1},$$

ここで，$m/2 \le i \le m$，ε は 0，1 または -1．

(iii) 適当な条件の下で，重みの小さい符号ベクトルはすべて，ある線形部分符号に属するといった形の若干の結果[8,9]．

(iv) 1次と2次のRM符号のWE，任意の次数のRM符号の $2.5\,d_{min}$（d_{min}：最小重み）より小さい重みについてのすべての A_i が知られている[10,11]．

(v) MacWilliams の等式を変形した Pless の等式[2]：

$$\sum_{i=0}^{n} (n-2i)^j A_i = 2^k \sum_{i=0}^{j} B_i F_j^{(i)}(n), \quad 0 \le j \le n$$

ここで，$F_j^{(i)}(n) = \frac{d^j}{dx^j}\left[\cosh^{n-i}x \sinh^i x\right]_{x=0}$

(vi) (i)～(v) および，BCH下界，Carlitz-Uchiyama 上界を使い，それ自身またはその双対符号の拡張符号が，2次RM符号の部分符号であるような巡回符号のいくつかのクラス（2重，3重誤り訂正BCH符号，最小重みが $2^{m-1}-2^{i-1}$ の形の符号長 2^m-1 のBCH符号，(0,2)次EG符号などを含む）について完全なWEが求められている[2,8,9]．

(vii) BCH符号の最小重み

長さ 2^m-1 の狭義BCH符号について，正確な最小重みは，多くの場合わかっていない．BCH下界と一致しない場合があることは知られている[1]．両者が一致するいくつかの十分条

件がわかっている.[1,2]

4. Justesen符号その他

Cを2^m元ν次RS等号とする．αをGF(2^m)の原始元とするとき，$v=(v_0,\cdots,v_{2^m-2})\in C$に対して，

$$v^J=(v_0,\alpha^0 v_0,v_1,\alpha^1 v_1,\cdots,v_i,\alpha^i v_i,\cdots,v_{2^m-2},\alpha^{2^m-2}v_{2^m-2})$$

とおく．すべての$v\in C$について，v^Jの各成分をGF(2)の上のm次元ベクトルによる表現でおきかえてえられる，長さ$2m(2^m-1)$の2元ベクトル全体をJustesen符号[14]という．符号長$n=2m(2^m-1)$，情報点数$k=m(2^m-2-\nu)$である．簡単な議論で，任意の$0<R<1/2$のRについて，各mに関し，$k/n\geq R$が成立するよう最大のνを選ぶとき，

$$\lim_{n\to\infty}\inf(d_{min}/n)\geq 0.11(1-2R)$$

Gilbert - Varsharmov下界[1,2]に比べるとかなり劣るが，"陽に"構成法が与えられた符号でk/nを一定にして，$n\to\infty$とするとき，$d_{min}/n\geq const>0$となる符号としては最初のものである．巡回符号のなかで，このような性質をもつ符号が"存在"するかどうか未解決である．$n=2^m-1$の巡回符号の拡張符号を考え，2^m個の成分の位置に，順に，$0,\alpha^0,\alpha^1,\cdots,\alpha^{2^m-2}$を対応させる．任意の$a\neq 0$，$b\in GF(2^m)$について変換，$X\to aX+b$に対応して，成分の位置が置換がきまるが，拡張符号

がこのような置換に不変であるとき，A-不変という．多項式符号（したがって，ＢＣＨ符号）やその双対符号はA-不変である．[1,2] A-不変な符号では，$K/n \approx$ 一定で，$n \to \infty$ のとき，$d_{min}/n \to 0$ となることが示されている．[12] この種の問題に関連して，興味をもたれているもう一つのクラスは，自己双対な符号であり，Gilbert-Varsharmov 下界の成立が知られている．[6] 自己双対符号のＷＥの形の制限から，d_{min}/n の上界，その上界を満す符号が存在するとしたときのＷＥを求めることなどが研究されている．[7]

文　献

(1) W.W. Peterson and E.J. Weldon, Jr.: "Error-correcting codes", Second Edition, MIT press, Cambridge, Mass. (1972).

(2) E.R. Berlekamp : "Algebraic coding theory", MacGraw-Hill, New York (1968).

(3) J.H. Van Lint : "Coding theory", Springer-Verlag, Berlin･Heidelberg･New York (1971).

(4) E.R. Berlekamp, F.J. MacWilliams and N.J.A. Sloane : "Gleason's theorem on self-dual codes", IEEE Trans., IT-18, p.409 (1972).

(5) F.J. MacWilliams, C.L. Mallows and N.J.A. Sloane : "Generalizations of Gleason's theorem on weight enumerators of self-dual codes", IEEE trans., IT-18, p.794 (1972).

(6) F.J. MacWilliams, N.J.A. Sloane and J.G. Thompson : "Good self-dual codes exist", Discrete Math., to appear.

(7) C.L. Mallows and N.J.A. Sloane : "An upper bound for self-dual codes", to appear.

(8) E.R. Berlekamp : "The weight enumerators for certain subcodes of the 2nd order binary Reed-Muller code", Inform. Control, Vol.17, p.485 (1970).

(9) T. Kasami : "The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes", Inform. Control, Vol.18, p.369 (1971).

(10) T. Kasami and N. Tokura : "On the weight structure of Reed-Muller codes", IEEE Trans., IT-16, p.752 (1970).

(11) 嵩忠雄·都倉信樹·安積三朗："Reed-Muller 符号の重み分布公式 ($2d \leq w < 2.5d$)"，信学会オートマトンと言語研資，AL-113 (1973-01).

(12) T. Kasami : "An upper bound on k/n for affine invariant codes with fixed d/n", IEEE Trans., IT-15, p.174 (1969).

(13) F.J. MacWilliams, N.J.A. Sloane and J.-M. Goethals : "The MacWilliams identities for nonlinear codes", B.S.T.J., Vol.51, p.803 (1972).

(14) J. Justesen : "A class of constructive asymptotically good algebraic codes", IEEE Trans., IT-18, 5, p.652 (1972).